U.S. Senate
Republican Policy
Committee

Legislative Notice

Jon Kyl, Chairman

No. 43 October 22, 2003

S. 877 – CAN-SPAM Act of 2003

Calendar No. 209

Reported by a voice vote on July 16, 2003, by the Committee on Commerce, Science, and Transportation, with an amendment in the nature of a substitute. S. Rept. 108-102.

Noteworthy

- The Senate began consideration of S. 877, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (CAN-SPAM Act) on October 22, 2003.

- S. 877 has bipartisan support: 11 of its 19 cosponsors are Democrats.

- S. 877 regulates the use of commercial e-mail, including Unsolicited Commercial E-Mail (UCE), more commonly known as "spam," and gives consumers the right to demand that a "spammer" cease sending them messages. The legislation creates civil and criminal penalties for spam if it is intended to deceive recipients as to its source or content; it imposes civil penalties for commercial e-mail that fails to include an "opt-out" mechanism; and it provides other consumer safeguards. Enforcement authority would rest with the Federal Trade Commission (FTC) while industry-specific regulatory authorities would bear some responsibilities.

Highlights

Federal Statutory Regime

The CAN-SPAM Act (the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003"), S. 877, would –

- give consumers the right to demand that a "spammer" (i.e., a sender of Unsolicited Commercial E-mail (UCE)) cease sending them messages;

- create civil and criminal sanctions for the sending of "spam" meant to deceive recipients as to its source or content;

- institute civil penalties for commercial e-mail that fails to include an "opt-out" mechanism (i.e., a way for consumers to no longer receive commercial e-mail from the sender.);

- provide other consumer safeguards, including clear and conspicuous identification that the e-mail is an advertisement;

- provide the FTC with the authority for enforcement of most of the provisions, while industry-specific regulatory authorities would bear some responsibilities as well; and

- authorize State attorneys general and Internet Service Providers (ISPs) to bring actions against violators.

Accurate Information Required of Spammers

- The bill would require senders of all commercial e-mail to include a valid return e-mail address and other header information with the message that accurately identifies the sender and Internet location from which the message has been sent.

- The bill also would require senders of UCE to provide an Internet-based system for consumers to opt out of receiving further messages from that sender. The bill provides an exception to that requirement – a "transactional or relationship message," which is defined in the bill as an electronic mail message, the primary purpose of which is to: facilitate, complete, or confirm a transaction; provide specified types of information with respect to a product or service used or purchased by the recipient; provide information directly related to a current employment relationship or benefit plan; or deliver goods or services that are included under the terms of a previous transaction.

- The bill would require a sender of spam to include in the e-mail message itself a valid physical address of the sender, as well as clear and conspicuous notice that both the message is an advertisement or solicitation and that the recipient may "opt out" of further UCE from the sender.

Additional Requirements on Businesses

- To ensure that businesses do not use e-mail sent with false or misleading transmission information to promote themselves, the bill would hold the promoted businesses responsible if they:

  1. know or should know about such deceptive promotion;
  2. are receiving or expect to receive an economic benefit from it; and
  3. are taking no reasonable precautions to prevent such promotion or to detect and report it to the FTC.

- Under the bill, senders of e-mail who intentionally disguise the source of their messages by falsifying header information could face criminal and civil sanctions. Civil sanctions would be available for other violations of the bill. The Judiciary Committee's anti-spam bill, S. 1293, takes a slightly different tack on such penalties.

Background

Unsolicited commercial e-mail (UCE), or spam, has become a great nuisance for many of the estimated 140 million Americans who regularly use e-mail for social or business purposes. The volume of spam has increased from 8 percent of all global e-mail traffic to 46 percent this year, according to the Federal Trade Commission. Worse, according to an April 2003 Federal Trade Commission (FTC) report entitled, *False Claims in Spam*, 66 percent of all spam contains some kind of false, fraudulent, or misleading information, either in the e-mail's routing information, its subject line, or the body of its message. The FTC also found that get-rich-quick opportunities and pornographic or adult-oriented material accounted for 38 percent of all spam.

Efforts have been made by some Internet Service Providers (ISPs) to block spam from subscribers' in-boxes, but this has proven costly and often futile. As of May 2003, two of the leading ISPs, America Online (AOL) and Microsoft (MSN and Hotmail), each/together were blocking 2.4 million spam messages a day. *USA Today* recently reported that more than 2 trillion spam messages are expected to be sent over the Internet this year, or 100 times the amount of direct mail advertising pieces delivered by U.S. mail last year.

While estimates of the cost of spam differ dramatically, *USA Today* reported in April that research organizations estimate that fighting spam adds an average of $2 per month to an individual's Internet bill. In addition to the costs to ISPs and consumers is the cost of spam to businesses and the economy. Ferris Research currently estimates that costs to U.S. businesses from spam in lost productivity, network system upgrades, unrecoverable data, and increased personnel costs, combined, will top $10 billion in 2003. Of this total, Ferris estimates that $4 billion is attributed to employee productivity losses from sifting through and deleting spam. Based on current spam growth rates, the Radicati Group estimates that, on a worldwide basis, spam could cost corporations over $113 billion by 2007.

Bill Provisions

Sections 1 – 3

Sections one through three of the bill consist of the title, Congressional findings regarding spam (a summary of which is provided in the preceding "Background" section), and statutory definitions of: "affirmative consent," "commercial electronic mail message," "electronic mail message," "header information," "implied consent," "initiate," "procure," "recipient," "sender," "transactional or relationship message," and "unsolicited commercial electronic mail message."

Section 4

Section 4 would amend chapter 63 of title 18, United States Code, to require that a person who sends commercial e-mail, with knowledge and intent that the message contains or is accompanied by header information that is materially false or materially misleading, shall be fined or imprisoned for up to one year, or both. This provision would also apply to spammers who hack into, or use false pretenses to obtain, an innocent party's e-mail account and use it to send out spam.

Section 5

This section provides a bevy of other protections for e-mail users and prescribes civil penalties enforceable under the FTC's pre-existing authority to regulate unfair or deceptive trade practices. The provisions (points 1-3 apply to all commercial e-mail, while points 4 and 5 only apply to spam) are as follows:

1. It would be unlawful to initiate a commercial e-mail message that contains or is accompanied by header information (source, destination and routing information – a.k.a. the "from" line) that is false or misleading.
2. It would prohibit spammers from **knowingly** using deceptive "subject" headings.
3. An entity that sends a commercial e-mail message must have a return e-mail address or other Internet-based reply mechanism that is operational for at least 30 days after the e-mail was sent. Exceptions are made for unforeseen technical difficulties. The sender must also provide a recipient with the option of declining to receive all further messages, although the sender could also give the recipient the option of receiving some types of messages but not others. The bill makes an exception for "transactional or relationship" e-mail messages (defined on p. 2 of this Notice).
4. Once a recipient requests not to receive any more spam from a specific sender, that sender (as well as any person acting on the sender's behalf, including any person who provides or selects e-mail addresses for the sender) must cease the transmission of spam to such recipient within 10 business days after receiving the request. In addition, it would be unlawful for anyone to sell or transfer the e-mail address of a recipient submitting an opt-out request. According to the Committee, "This is intended to prevent a sender or other person from treating

an opt-out request as a confirmation of a 'live' e-mail address, and selling that information to other would-be spammers."

5. Any spam would be required to contain: clear and conspicuous identification that the e-mail is an advertisement or solicitation; clear and conspicuous notice of the opportunity to decline receiving further UCE; and the inclusion of a valid physical postal address for the sender.
6. Four "aggravated violations" would trigger more severe penalties: obtaining e-mail addresses from websites with explicit policies that disavow the sale or transfer of e-mail addresses; obtaining e-mail addresses from automated means that generate potential e-mail addresses using combination of names, letters, and numbers; automated account creation, where a spammer opens a significant number of temporary, Internet-based, free accounts he uses to spam; and retransmission through computers with unauthorized access.

Section 6

Section 6, added by Chairman McCain and unanimously supported at the Committee markup, permits the FTC (but not State AG's or ISPs) to use an alternative way to enforce one category of violations in the bill – the use of false headers. Without section 6, the FTC would be required under section 5 to first determine the identity of the actual person who sent out a false-header e-mail and then prove a nexus between that sender and the company promoted in that e-mail to address the promoted company's violations.

The FTC claims this evidentiary burden is too great to allow the agency to enforce the provision, especially in the situation of false-header e-mail where the actual identity of the spammer is unknown and usually untraceable. Thus, without section 6, there could be a major niche exploited by professional, high-volume spammers who run massive, commission-based spam campaigns using false-header e-mails.

To address this weakness, section 6 would permit the FTC to instead enforce the Section 5 provision directly against the company promoted in a false-header e-mail provided three conditions are met:

(1) the promoted entity knows or should know it is being promoted in a false header e-mail;
(2) the entity is receiving or expects to receive an economic benefit from such promotion, and;
(3) the entity is taking no reasonable precautions to prevent it, or to detect and report it to the FTC.

The third provision is an important safeguard to give legitimate companies who do not spam an opportunity to proactively avoid mistaken FTC action if they have been victimized by "spoofed sender" spam – unauthorized messages sent using their name as the sender in order to bypass ISP filters, trick consumers into opening the e-mail message, and/or sell counterfeited goods.

Section 7

This section reiterates that the FTC would enforce Section 5 of this Act under section 18 of the FTC Act (15 U.S.C. 41 et seq.) as if the violation were an unfair or deceptive act or practice and that all the jurisdictional, remedial, and civil enforcement provisions of the FTC Act would be applicable to commercial e-mail. Due to the jurisdictional limitations of the FTC Act, several other agencies also would play a role in enforcement, including the Federal Reserve Board, the Office of the Comptroller of the Currency, the Farm Credit Administration, and other industry-specific regulators.

This section also would grant State attorneys general or affected ISPs the right to bring a civil action for violations of section 5. A State may bring an action in *parens patriae* for aggrieved citizens of the State in Federal district court or other court of competent jurisdiction to obtain injunctive relief or recover actual or statutory damages, whichever is greater. Statutory damages under this section are up to $100 per message with falsified header information; or $25 per message that is otherwise unlawful under this legislation, up to a cap of $1 million. These amounts could be tripled under the "aggravated violations" provisions mentioned in Section 5.

Section 8

This section makes clear that nothing in this Act should be understood to affect the provisions of the Communications Act of 1934 or the legality of ISPs' efforts to filter or block e-mails on their systems. The section also makes clear that any state law dealing specifically with spam would be preempted, but those that do not expressly regulate e-mail, or prohibit fraud carried out via e-mail would not be preempted.

Section 9

This section instructs the FTC to complete a plan for creating a "Do-Not-E-mail List" within six months of implementing its "Do-Not-Call List" or explain why such a list would be infeasible.

Section 10

This Section instructs the FTC, in consultation with the Justice Department and other relevant agencies, to submit a report to Congress within 24 months of the date of enactment of this bill that analyzes the effectiveness and enforcement of this legislation, and considers what steps could be taken to improve it, particularly in the international context, and in further protecting children from pornographic spam.

Section 11

This section states that if any provision or application of a provision of the legislation is held invalid, the remainder of the legislation and application of its provisions would not be affected.

Section 12

This section provides that the provisions of this legislation would take effect 120 days after the date of enactment.

Administration Position

No Administration position was available as of press time.

Cost

CBO estimates that implementing S. 877 would cost about $1 million in 2004 and about $2 million a year in 2005 and thereafter, assuming appropriation of the necessary amounts. CBO estimates that civil penalties collected as a result of enacting this bill would increase governmental receipts (revenues) by about $3 million a year when fully implemented (by 2005). The bill also would have additional effects on revenues and direct spending by imposing costs on banking regulators and by creating new penalties. However, CBO estimates that those additional effects would be negligible.

Possible Amendments

Burns/Wyden. To make technical corrections related to clarifying certain provisions of the bill as reported; harmonize the civil and criminal provisions of the bill regarding materiality standards.

Schumer. To establish a process for Congressional consideration of a nationwide Do-Not-E-mail registry proposal.

Santorum. To: (i) add a safe harbor for compliance with self-regulatory programs, and (ii) add criminal penalties for failure to label sexually explicit spam.

Hatch/Leahy. To replace S. 877's criminal enforcement provisions with those of S. 1293, as reported.